

How to Pen Test an ATM

BREAKING INTO NETWORK-CONNECTED BOXES OF CASH



Who am I?

- Daniel Crowley
- Research Baron at X-Force Red
- Pen tester since 2004
- Locksport enthusiast and past competition winner
- Actually holds the title of Baron (in Sealand)

Why ATMs?

- Cash-filled safe
- Windows box
- Combination cash-filled safe and Windows box
- Requires WAN connection
- Always on
- Always logged in
- Available to the public

Components of an ATM



PHYSICAL



Locks

- Crap default wafer locks
- Crap default tubular locks
- Small number of possible default keys
- Lock mechanisms independent of tumbler state
- Alternative entry points

Default keys



Hantle GenMega ATM Machine N

You are considering a new Hantle/Genme G2500 and Onyx GT3000.

\$7.99

\$3.00 shipping

2 new & refurbished from \$7.99

CH751



Which would win?



Which would win?



Safe

- Default entry code
- Holes
 - Dispenser
 - Power cabling
 - Network cabling
 - Serial cabling

Assorted tomfoolery

- Optical bill sensor
- Direct actuation of dispenser motors
- Hardware hax
 - JTAG/UART
 - SPI flashing

NETWORK



Encryption

- No encryption
- Fixed encryption key
- Replay attacks
- Limitations of mainframe (yes, mainframe) processing power

Exposed network gear



Usual network shenanigans



ATM networks

- Modems (wired or cellular)
- Ethernet
- Compromising one may allow lateral attacks
 - ...or attacks against ATM infrastructure

Real world attack



APPLICATION



Management applications

- Casino ATMs
 - Gaming server
 - Voucher scanner
- Remote management

Kiosk application

- Kiosk breakout
 - Power up time
 - Touching randomly around the screen
- Management mode
 - Enter+clear+cancel, 1, 2, 3
 - Default codes
 - Any digit * 6
 - 123456
 - Management card

Network comms attack surface

- Open ports aren't the final word!

OPERATING SYSTEM





Old OS versions

- MS08-067
- MS17-010

Misconfiguration

- NBNS/LLMNR
- WPAD
- Unencrypted hard drive

Passwords

- Weak or default passwords
- Same local admin passwords across multiple ATMs

Hotkeys

- Alt+Tab
- Win+Tab
- Ctrl+Alt+Del
- Win+E
- Win+D
- etc



DANIEL.CROWLEY1@IBM.COM






QUESTIONS?





THANK YOU

FOLLOW US ON:

-  ibm.com/security
-  securityintelligence.com
-  xforce.ibmcloud.com
-  [@ibmsecurity](https://twitter.com/ibmsecurity)
-  youtube/user/ibmsecuritysolutions

© Copyright IBM Corporation 2016. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, these materials. Nothing contained in these materials is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software. References in these materials to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and / or capabilities referenced in these materials may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective.

IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

